JC564 U.S. PTO
09/504020
02/14/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants : Masayuki TERADA et al.

Serial No. : To Be Assigned

Filed : Herewith

For : ORIGINAL DATA CIRCULATION METHOD, SYSTEM, APPARATUS, AND COMPUTER READABLE MEDIUM

Assistant Commissioner for Patents
Washington, D.C. 20231

CLAIM TO CONVENTION PRIORITY UNDER 35 U.S.C. 119

S I R :

A claim to the Convention Priority Date of each of the following Japanese Patent Applications is being made at the time this United States application is being filed.

Application No.	Filed
11-039080	February 17, 1999
11-247457	September 1, 1999

In order to complete the claim to Convention Priority Dates under 35 U.S.C. 119, a certified copy of each of these Japanese applications is enclosed herewith.

Respectfully submitted,

KENYON & KENYON

By _____
Edward W. Greason
Reg. No. 18,918

One Broadway
New York, N.Y. 10004
(212) 425-7200
Dated: February 14, 2000
EXPRESS MAIL EL039790667US

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: September 1, 1999

Application Number: Japanese Patent Application No. 11-247457

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE CORPORATION

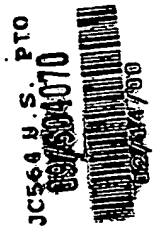
January 14, 2000

Commissioner,
Patent Office Takahiko Kondo (Seal)

Certificate No.11-3094228

Express Mail EL039790667US.

PATENT OFFICE
JAPANESE GOVERNMENT



This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: February 17, 1999

Application Number: Japanese Patent Application No. 11-039080

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE CORPORATION

January 14, 2000

Commissioner,
Patent Office Takahiko Kondo (Seal)

Certificate No.11-3094216

Express Mail EL039790667US

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ２月１７日

出 願 番 号
Application Number: 平成１１年特許願第０３９０８０号

出 願 人
Applicant (s): 日本電信電話株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 １月１４日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆

【書類名】　特許願

【整理番号】　NTTH106951

【提出日】　平成11年 2月17日

【あて先】　特許庁長官　伊佐山　建志　殿

【国際特許分類】　G06F 13/38

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　寺田　雅之

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100070150

【弁理士】

【氏名又は名称】　伊東　忠彦

【手数料の表示】

【予納台帳番号】　002989

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ蓄積方法及びシステム及びデータ蓄積プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項１】　価値を有する電子的な情報の蓄積を行うデータ蓄積方法において、

電子的な情報の発行者装置により該電子的な情報に署名した第１の情報を付与し、

前記発行者装置により前記電子的な情報と対応するマニフェストの第２の情報を生成して、前記第１の情報に付与し、

電子的な情報利用装置において、前記第１の情報と前記第２の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止することを特徴とするデータ蓄積方法。

【請求項２】　電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得し、

前記情報利用装置において、前記検証鍵からセッション情報を生成し、

前記セッション情報の正当性を判定する請求項１記載のデータ蓄積方法。

【請求項３】　前記第２の情報を耐タンパ性の装置に格納し、前記発行者装置の同一性を判定し、前記電子的な情報の複製を防止する請求項１記載のデータ蓄積方法。

【請求項４】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

電子的な情報に署名した第１の情報を付与し、該電子的な情報と対応するマニフェストの第２の情報を生成して、前記第１の情報に付与する発行者装置と、

前記第１の情報と前記第２の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止する利用者装置とを有することを特徴とするデータ蓄積システム。

【請求項５】　前記利用者装置は、

電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得する手

段を有し、

前記検証鍵からセッション情報を生成する手段と、

前記セッション情報の正当性を判定する手段を有する改札装置を更に有する請求項４記載のデータ蓄積システム。

【請求項６】　前記利用者装置は、

前記第２の情報を耐タンパ性の装置に格納し、前記発行者装置の同一性を判定する手段を含む請求項４記載のデータ蓄積システム。

【請求項７】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第１の署名手段と、

前記署名が付与された情報の格納及び抽出を行うための第１の格納手段と、

前記電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第２の格納手段と、

前記電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第１の認証手段と、

前記署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を前記第１の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが前記第１の認証手段により検証された時のみ、該マニフェストを前記第２の格納手段に格納する第１の制御手段とを有する利用者装置を有することを特徴とするデータ蓄積システム。

【請求項８】　前記利用者装置の前記第２の格納手段及び前記第１の認証手段は、耐タンパ性を有する請求項７記載のデータ蓄積システム。

【請求項９】　前記第１の認証手段は、

前記第１の格納手段に格納された前記署名が付与された情報の有効性を、該情報と対応するマニフェストが前記第２の格納手段に格納されているか否かにより検証し、該マニフェストが該第２の格納手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第２の格納手段に格納されていなかったときには、該情報を無効とする手段を含む請求項７記載のデータ蓄積システム。

【請求項１０】　前記電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第２の署名手段と、

マニフェストの格納及び抽出を行う第３の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第２の認証手段と、

ある電子的な情報に対応するマニフェストを前記第２の格納手段から前記第３の格納手段に移動させる際に、該第２の格納手段から該マニフェストを抽出し、前記第２の署名手段により該マニフェストに署名を付与し、該第２の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第２の認証手段により検証し、検証に成功した時のみ前記第３の格納手段に該マニフェストを格納する第２の制御手段とを有する発行者装置を有する請求項７記載のデータ蓄積システム。

【請求項１１】　前記発行者装置の前記第３の格納手段、第２の署名手段、前記第２の認証手段が耐タンパ性を有する請求項１０記載のデータ蓄積システム。

【請求項１２】　システム内で一意性を持つセッション情報を生成するセッション情報生成手段と、

前記セッション情報の格納及び抽出を行うための第４の格納手段とを具備する改札装置を更に有し、

前記改札装置は、

ある電子的な情報に対応するマニフェストを前記利用者装置の前記第２の格納手段から前記発行者装置の前記第３の格納手段に移動させる際に、前記セション情報生成手段によりセッション情報を生成し、前記第４の格納手段に該セッション情報を格納し、

前記利用者装置は、

前記第２の格納手段から前記マニフェストを抽出し、

前記発行者装置は、

前記第２の署名手段により該マニフェストと該セッション情報の組に署名を付与し、該第２の格納手段から該マニフェストを削除し、該組の署名者を該電子的な情報の署名者が信用することを前記第２の認証手段により認証し、

前記改札装置は、

前記第２の認証手段において認証が成功し、かつ、該組に含まれるセッション情報が、前記第４の格納手段に格納されていたときのみ、該第４の格納手段から該セッション情報を削除し、

前記発行者装置は、

前記第３の格納手段に前記マニフェストを格納する請求項７及び１０記載のデータ蓄積システム。

【請求項１３】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第１の署名手段と、

前記署名が付与された情報の格納及び抽出を行うための第１の格納手段と、

前記電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第２の格納手段と、

前記電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第１の認証手段と、

前記署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を前記第１の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが前記第１の認証手段により検証された時のみ、該マニフェストを前記第２の格納手段に格納する第１の制御手段とを有する利用者装置と、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第２の署名手段と、

マニフェストの格納及び抽出を行う第３の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第２の認証手段と、

ある電子的な情報に対応するマニフェストを前記第２の格納手段から前記第３の格納手段に移動させる際に、該第２の格納手段から該マニフェストを抽出し、前記第２の署名手段により該マニフェストに署名を付与し、該第２の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第２の認証手段により検証し、検証に成功した時のみ前記第３の格納手段に該マニフェストを格納する第２の制御手段とを有する発行者装置とを有することを特徴とするデータ蓄積システム。

【請求項１４】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第１の署名手段と、

前記署名が付与された情報の格納及び抽出を行うための第１の格納手段と、

前記電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第２の格納手段と、

前記電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第１の認証手段と、

前記署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を前記第１の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが前記第１の認証手段により検証された時のみ、該マニフェストを前記第２の格納手段に格納する第１の制御手段とを有する利用者装置と、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第２の署名手段と、

マニフェストの格納及び抽出を行う第３の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に

含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第２の認証手段と、

ある電子的な情報に対応するマニフェストを前記第２の格納手段から前記第３の格納手段に移動させる際に、該第２の格納手段から該マニフェストを抽出し、前記第２の署名手段により該マニフェストに署名を付与し、該第２の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを前記第２の認証手段により検証し、検証に成功した時のみ前記第３の格納手段に該マニフェストを格納する第２の制御手段とを有する発行者装置と、

システム内で一意性を持つセッション情報を生成するセッション情報生成手段と、

前記セッション情報の格納及び抽出を行うための第４の格納手段とを具備する改札装置を具備し、

前記利用者装置は、

前記第２の格納手段から前記マニフェストを抽出し、

前記発行者装置は、

前記第２の署名手段により該マニフェストと該セッション情報の組に署名を付与し、該第２の格納手段から該マニフェストを削除し、該組の署名者を該電子的な情報の署名者が信用することを前記第２の認証手段により認証し、

前記改札装置は、

前記第２の認証手段において認証が成功し、かつ、該組に含まれるセッション情報が、前記第４の格納手段に格納されていたときのみ、該第４の格納手段から該セッション情報を削除し、

前記発行者装置は、

前記第３の格納手段に前記マニフェストを格納することを特徴とするデータ蓄積システム。

【請求項１５】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

電子的な情報に署名した第１の情報を付与し、該電子的な情報と対応するマニフェストの第２の情報を生成して、前記第１の情報に付与するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項１６】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

前記第１の情報と前記第２の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するプロセスを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項１７】　電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得するプロセスと、

前記検証鍵からセッション情報を生成するプロセスと、

前記セッション情報の正当性を判定するプロセスを含む請求項１６記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項１８】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

生成者を特定可能な情報である署名を電子情報に付与する第１の署名プロセスと、

前記署名が付与された情報を第１の記憶手段に格納すると共に、抽出を行うための第１の格納プロセスと、

前記電子的な情報と１対１に対応するマニフェストを第２の記憶手段に格納すると共に、抽出を行うための第２の格納プロセスと、

前記電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第１の認証プロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項１９】　前記第１の認証プロセスは、

前記第１の記憶手段に格納された前記署名が付与された情報の有効性を、該情

報と対応するマニフェストが前記第２の記憶手段に格納されているか否かにより検証し、該マニフェストが該第２の記憶手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第２の記憶手段に格納されていなかったときには、該情報を無効とするプロセスを含む請求項１８記載のデータ蓄積プログラムを格納した記憶媒体。

【請求項２０】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

前記電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成プロセスと、

マニフェストに、署名を付与するための第２の署名プロセスと、

マニフェストを第３の記憶手段に格納すると共に、抽出を行う第３の格納プロセスと、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、前記情報の署名者とが同一であることを検討する第２の認証プロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【請求項２１】　価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける改札装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

システム内で一意性を持つセッション情報を生成するセッション情報生成プロセスと、

前記セッション情報を第４の記憶手段に格納すると共に抽出を行うための第４の格納プロセスとを有することを特徴とするデータ蓄積プログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ蓄積方法及びシステム及びデータ蓄積プログラムを格納した

記憶媒体に係り、特に、電子チケットなどの権利を表象するデータやディジタル著作物など、有効な複製数を一定以下に保つことが必要とされるデータについて、蓄積や配送のための手段を提供するためのデータ蓄積方法及びシステム及びデータ蓄積プログラムを格納した記憶媒体に関する。

【０００２】

【従来の技術】

権利を表象したデータや著作物などは、配布者などの意図する数を越えて同時に複製が存在することを防止することが求められる。即ち、配布したデータが利用者などにより複製され、それらが多重に利用されることを防ぐ必要がある。

従来は、以下で示すような技術によりそのような多重利用を防止している。

【０００３】

第１の方法として、権利を表象するデータについて、権利の提供者などにより、当該データの使用履歴を保持しておき、権利の行使時に、当該データが既に使用されていないかどうかを検証する。もし、既に使用されていれば、当該データが表象する権利の行使を拒否する。

第２の方法として、データ自身を耐タンパ装置に格納し、当該データを当該耐タンパ装置以外からは参照できないようにする。権利の行使時には、当該データを該耐タンパ装置より抹消する。

【０００４】

【発明が解決しようとする課題】

しかしながら、上記従来の第１の方法では、耐タンパ装置などの特別な装置を必要としていないが、データを転々流通させる際に問題が生じる。即ち、当該技術では、行使時の事後検出しか行えないため、流通過程では、当該データの有効性は判定できないという問題がある。

【０００５】

従来の第２の方法では、耐タンパ装置を用いることにより、データの唯一性を保証することができる。また、（特願平６－５０３９１３）や、（特開平９－５１１３５０）などで述べられている方式などを併用し、暗号によって保護された安全な通信路を介して耐タンパ装置を結合し、当該通信路を介してデータの授受

を行うことにより、当該データの流通を、複製を事前に防止しながら行うことを可能とする。しかしながら、当該技術は、耐タンパ装置の中にデータを格納する必要があるため、以下の２点が問題となる。

【０００６】

まず、データの記述そのものを見ることができなくなるため、記述の正当性の検証など、複製に関する有効性以外の検証も全て当該耐タンパ装置に委ねなければならないという制約が生じる。

また、データの格納部のみならず、データの取扱に必要な処理も全て耐タンパ装置が負わなければならないため、耐タンパ装置に対して記憶容量や処理速度に大きな要求が発生する。特に、現時点で耐タンパ装置として一般的なＩＣカードでは、処理速度や記憶容量に不足が生じる。

【０００７】

本発明は、上記の点に鑑みなされたもので、データの有効な複製数を一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証をすべて耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させるデータ蓄積方法及びシステム及びデータ蓄積プログラムを格納した記憶媒体を提供することを目的とする。

【０００８】

【課題を解決するための手段】

図１は、本発明の原理を説明するための図である。

本発明（請求項１）は、価値を有する電子的な情報の蓄積を行うデータ蓄積方法において、

電子的な情報の発行者装置により該電子的な情報に署名した第１の情報を付与し（ステップ１）、

発行者装置により電子的な情報と対応するマニフェストの第２の情報を生成して、第１の情報に付与し（ステップ２）、

電子的な利用者装置において、第１の情報と第２の情報を用いて電子的な情報の発行者装置の同一性を判定し（ステップ３）、電子的な情報の複製を防止する。

【０００９】

本発明（請求項２）は、電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得し、

利用者装置において、検証鍵からセッション情報を生成し、

セッション情報の正当性を判定する。

本発明（請求項３）は、第２の情報を耐タンパ性の装置に格納し、発行者装置の同一性を判定し、電子的な情報の複製を防止する。

【００１０】

図２は、本発明の原理構成図である。

本発明（請求項４）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

電子的な情報に署名した第１の情報を付与し、該電子的な情報と対応するマニフェストの第２の情報を生成して、第１の情報に付与する発行者装置１と、

第１の情報と第２の情報を用いて電子的な情報の発行者装置１の同一性を判定し、電子的な情報の複製を防止する利用者装置２とを有する。

【００１１】

本発明（請求項５）は、上記のシステムにおいて、

利用者装置２は、電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得する手段を有し、

検証鍵からセッション情報を生成する手段と、

セッション情報の正当性を判定する手段を有する改札装置を更に有する。

【００１２】

本発明（請求項６）は、利用者装置２において、

第２の情報を耐タンパ性の装置に格納し、発行者装置の同一性を判定する手段を含む。

本発明（請求項７）は、生成者を特定可能な情報である署名を電子情報に付与する第１の署名手段と、　署名が付与された情報の格納及び抽出を行うための第１の格納手段と、

電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第

２の格納手段と、

電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第１の認証手段と、

署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を第１の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが第１の認証手段により検証された時のみ、該マニフェストを第２の格納手段に格納する第１の制御手段とを有する利用者装置を有する。

【００１３】

本発明（請求項８）は、利用者装置の第２の格納手段及び第１の認証手段において、耐タンパ性を有する。

本発明（請求項９）は、第１の認証手段において、

第１の格納手段に格納された署名が付与された情報の有効性を、該情報と対応するマニフェストが第２の格納手段に格納されているか否かにより検証し、該マニフェストが該第２の格納手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第２の格納手段に格納されていなかったときには、該情報を無効とする手段を含む。

【００１４】

本発明（請求項１０）は、電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第２の署名手段と、

マニフェストの格納及び抽出を行う第３の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、情報の署名者とが同一であることを検討する第２の認証手段と、

ある電子的な情報に対応するマニフェストを第２の格納手段から第３の格納手段に移動させる際に、該第２の格納手段から該マニフェストを抽出し、第２の署

名手段により該マニフェストに署名を付与し、該第２の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを第２の認証手段により検証し、検証に成功した時のみ第３の格納手段に該マニフェストを格納する第２の制御手段とを有する発行者装置を有する。

【００１５】

本発明（請求項１１）は、発行者装置の第３の格納手段、第２の署名手段、第２の認証手段が耐タンパ性を有する。

本発明（請求項１２）は、システム内で一意性を持つセッション情報を生成するセッション情報生成手段と、

セッション情報の格納及び抽出を行うための第４の格納手段とを具備する改札装置を更に有し、

改札装置において、

ある電子的な情報に対応するマニフェストを利用者装置の第２の格納手段から発行者装置の第３の格納手段に移動させる際に、セション情報生成手段によりセッション情報を生成し、第４の格納手段に該セッション情報を格納し、

利用者装置において、

第２の格納手段からマニフェストを抽出し、

発行者装置において、

第２の署名手段により該マニフェストと該セッション情報の組に署名を付与し、該第２の格納手段から該マニフェストを削除し、該組の署名者を該電子的な情報の署名者が信用することを第２の認証手段により認証し、

改札装置において、

第２の認証手段において認証が成功し、かつ、該組に含まれるセッション情報が、第４の格納手段に格納されていたときのみ、該第４の格納手段から該セッション情報を削除し、

発行者装置において、

第３の格納手段にマニフェストを格納する。

【００１６】

本発明（請求項１３）は、価値を有する電子的な情報の蓄積を行うデータ蓄積

システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第１の署名手段と、

署名が付与された情報の格納及び抽出を行うための第１の格納手段と、

電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第２の格納手段と、

電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第１の認証手段と、

署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を第１の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが第１の認証手段により検証された時のみ、該マニフェストを第２の格納手段に格納する第１の制御手段とを有する利用者装置と、

電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第２の署名手段と、

マニフェストの格納及び抽出を行う第３の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、情報の署名者とが同一であることを検討する第２の認証手段と、

ある電子的な情報に対応するマニフェストを第２の格納手段から第３の格納手段に移動させる際に、該第２の格納手段から該マニフェストを抽出し、第２の署名手段により該マニフェストに署名を付与し、該第２の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを第２の認証手段により検証し、検証に成功した時のみ第３の格納手段に該マニフェストを格納する第２の制御手段とを有する発行者装置とを有する。

【００１７】

本発明（請求項１４）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムであって、

生成者を特定可能な情報である署名を電子情報に付与する第１の署名手段と、

署名が付与された情報の格納及び抽出を行うための第１の格納手段と、

電子的な情報と１対１に対応するマニフェストの格納及び抽出を行うための第２の格納手段と、

電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第１の認証手段と、

署名手段により署名が付与された署名付き情報を格納する際に、該署名付き情報を第１の格納手段に格納すると共に、該署名の署名者と該署名付き情報に対応するマニフェストの格納者とが同一であることが第１の認証手段により検証された時のみ、該マニフェストを第２の格納手段に格納する第１の制御手段とを有する利用者装置と、

電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成手段と、

マニフェストに、署名を付与するための第２の署名手段と、

マニフェストの格納及び抽出を行う第３の格納手段と、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び該信任情報の署名者と、情報の署名者とが同一であることを検討する第２の認証手段と、

ある電子的な情報に対応するマニフェストを第２の格納手段から第３の格納手段に移動させる際に、該第２の格納手段から該マニフェストを抽出し、第２の署名手段により該マニフェストに署名を付与し、該第２の格納手段から該マニフェストを削除し、該マニフェストの署名者を該電子的な情報の署名者が信用することを第２の認証手段により検証し、検証に成功した時のみ第３の格納手段に該マニフェストを格納する第２の制御手段とを有する発行者装置と、

システム内で一意性を持つセッション情報を生成するセッション情報生成手段と、

セッション情報の格納及び抽出を行うための第４の格納手段とを具備する改札装置を具備し、

利用者装置において、

第２の格納手段からマニフェストを抽出し、

発行者装置において、

第２の署名手段により該マニフェストと該セッション情報の組に署名を付与し、該第２の格納手段から該マニフェストを削除し、該組の署名者を該電子的な情報の署名者が信用することを第２の認証手段により認証し、

改札装置において、

第２の認証手段において認証が成功し、かつ、該組に含まれるセッション情報が、第４の格納手段に格納されていたときのみ、該第４の格納手段から該セッション情報を削除し、

発行者装置において、

第３の格納手段にマニフェストを格納する。

【００１８】

本発明（請求項１５）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

電子的な情報に署名した第１の情報を付与し、該電子的な情報と対応するマニフェストの第２の情報を生成して、第１の情報に付与するプロセスを有する。

【００１９】

本発明（請求項１６）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

第１の情報と第２の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止するプロセスを有する。

【００２０】

本発明（請求項１７）は、電子的な情報の発行を厳重に管理されたサーバの発行する検証鍵を取得するプロセスと、

検証鍵からセッション情報を生成するプロセスと、

セッション情報の正当性を判定するプロセスを含む。

本発明（請求項１８）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける利用者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

生成者を特定可能な情報である署名を電子情報に付与する第１の署名プロセスと、

署名が付与された情報を第１の記憶手段に格納すると共に、抽出を行うための第１の格納プロセスと、

電子的な情報と１対１に対応するマニフェストを第２の記憶手段に格納すると共に、抽出を行うための第２の格納プロセスと、

電子的な情報に付与された署名の生成者である署名者と該電子的な情報に対応するマニフェストを格納しようとする格納者とが同一であることを検証するための第１の認証プロセスとを有する。

【００２１】

本発明（請求項１９）は、第１の認証プロセスは、

第１の記憶手段に格納された署名が付与された情報の有効性を、該情報と対応するマニフェストが第２の記憶手段に格納されているか否かにより検証し、該マニフェストが該第２の記憶手段に格納されていたときのみ該情報が有効であるとし、該マニフェストが該第２の記憶手段に格納されていなかったときには、該情報を無効とするプロセスを含む。

【００２２】

本発明（請求項２０）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける発行者装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

電子的な情報の署名者が信用する署名者を指定する信任対象の１つまたは複数の集合からなる信任情報を生成する信任情報生成プロセスと、

マニフェストに、署名を付与するための第２の署名プロセスと、

マニフェストを第３の記憶手段に格納すると共に、抽出を行う第３の格納プロセスと、

マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に

含まれること、及び該信任情報の署名者と、情報の署名者とが同一であることを検討する第２の認証プロセスとを有する。

【００２３】

本発明（請求項２１）は、価値を有する電子的な情報の蓄積を行うデータ蓄積システムにおける改札装置に搭載されるデータ蓄積プログラムを格納した記憶媒体であって、

システム内で一意性を持つセッション情報を生成するセッション情報生成プロセスと、

セッション情報を第４の記憶手段に格納すると共に抽出を行うための第４の格納プロセスとを有する。

【００２４】

上記のように、本発明によれば、データ及び当該データに対応する署名を格納し、データと１対１に対応する情報であるマニフェストを格納し、署名の生成者でえある署名者を特定し、マニフェストを格納しようとする者が署名者と同一であるかどうかを検証することにより、署名者の意図した数のマニフェストがデータ蓄積システム内に格納される。

【００２５】

また、耐タンパ装置を用いることにより、データをデータ蓄積システム以外に格納することが可能となる。

また、データに対応するマニフェストがデータ蓄積システムに格納されている時のみ、当該データが有効であると区別することにより、マニフェストの数を越えて有効なデータが存在することを防止する。

【００２６】

また、データの署名者が信用する署名者である信任対象を指定し、マニフェストに、データ蓄積システムを署名者とする署名を付与し、マニフェストの署名者が信任対象または、信任対象がさらに信用する署名者に含まれること、及び信任情報の署名者と、データの署名者とが同一であることを検証する。これにより、当該データの署名者が信用する経路のみを介してマニフェストを移送することが可能となる。

【００２７】

さらに、このとき、耐タンパ装置を利用することにより、耐タンパ性が保証される。

また、システム内で一意性を持つセッション情報を生成し、セッション情報を格納することにより、暗号化された通信路を介することなく、１つのマニフェストが複数の格納部に格納されることを防止することが可能となると共に、複数のマニフェストを１つの格納部に並行に転送することが可能となる。

【００２８】

【発明の実施の形態】

図３は、本発明のデータ蓄積システムの全体構成を示す。同図では、権利を表象する電子情報である電子チケットをデータとして発行者が利用者に発行し、チケットを発行された利用者が別の利用者間に譲渡し、チケット譲渡された利用者がチケットを消費する際に、検証者がチケットの有効性を検証する場合を示している。

【００２９】

同図において、チケットの発行者は、発行者装置１を有し、チケットの発行先となる利用者は利用者装置２を有している。チケットの発行の際には、発行者装置１と利用者２の間は、接続装置４を介して通信手段が確立される。この通信手段は、発行の開始から終了までの間のみ確立されていればよい。

また、チケット譲渡の際には、発行時と同様に利用者装置２間で接続装置４を介して通信手段を確立し、チケットを利用者装置２間で転送する。チケットの改札者は、改札者装置３を有している。チケット改札の際には、発行時と同様に、利用者装置２と改札者装置３との間で接続装置４を介して、通信手段を確立し、改札者装置３にチケットを転送する。

【００３０】

チケット改札者は、改札者装置３を有している。チケットの改札の際には、発行時と同様に利用者装置２と改札者装置３との間で接続装置４を介して通信手段を確立し、改札者装置３にチケットを転送する。

このように、本発明にかかるデータ蓄積システムは、一時的な相互通信手段を

提供する接続装置４により接続された、１乃至複数の発行者装置１と、１乃至複数の利用者装置２と、１乃至複数の改札者装置３とから構成されるシステムである。

【００３１】

【実施例】

以下、図面と共に本発明の実施例を説明する。

ここで、図４から図７を用いて、上記データ蓄積システムを構成する各装置について説明する。以下に、説明で用いる式の意味を示す。

ｘ‖ｙとは、ｘとｙの連接である。

【００３２】

Ｈとは、一方向のハッシュ関数であり、ｙ＝Ｈ（ｘ）を満たすようなｘをｙから求めることが困難であるという性質を持つ。このようなハッシュ関数として、米ＲＳＡ社のＭＤ５などが知られている。

S_{Pk}とは、検証関数V_{Pk}により検証可能な電子署名を生成する署名関数である。

【００３３】

V_{Pk}は、検証関数であり、V_{Pk}（ｘ‖S_{Pk}（ｘ））＝１，V_{Pk}（ｏｔｈｅｒ）＝０という性質を持つ。即ち、ある情報ｘが署名関数S_{Pk}により署名されたものであるかどうかを検証できる性質を持つ。

Ｐｋは、検証鍵であり、検証器Ｖに検証鍵Ｐｋを与えることにより、V_{Pk}を構成することが可能であるという性質を持つ。署名が付与された検証鍵Ｐｋ２‖S_{Pk1}（Ｐｋ２）を特に、Ｐｋ１によるＰｋ２の鍵証明書と呼ぶ。

【００３４】

以上で述べたような性質を持つS_{Pk}、V_{Pk}を実現するような電子署名方式として、日本電信電話のＥＳＩＧＮなどが知られている。

図４は、本発明の一実施例の発行者装置の構成を示す。

同図に示す発行者装置１は、制御部１１、署名部１２、データ生成部１３、マニフェスト生成部１４、信任情報生成部１５から構成される。

【００３５】

制御部１１は、検証鍵ＰｋＩを保持し、チケットの流通を安全に行うための制御を行う。ここで、ＰｋＩは後述する署名部１２が備える署名関数S_{PkI}に対応する検証鍵である。制御部１１による制御の詳細については後述する。

署名部１２は、署名関数S_{PkI}を備える。署名関数S_{PkI}は、発行者装置１毎にそれぞれ異なり、署名部１２により秘匿される。

【００３６】

データ生成部１３は、内部で生成した情報に基づいて、もしくは、外部から与えられた情報に基づいて、データｍを生成する。本発明に係るデータ蓄積システムでは、データｍの記述内容についてなんら制限を持つものではないため、データｍとして切符やコンサートチケットなどの一般的なチケットによって扱われる権利を表象する電子情報の他、プログラム、音楽、画像データなどを扱うことが可能である。

【００３７】

マニフェスト生成部１４は、一方向のハッシュ関数Ｈを備え、署名付きデータ$m \| S_{PkI(m)}$のマニフェスト$c_{(m,PkI)} = H(m \| S_{PkI(m)})$を生成する。

信任情報生成部１５は、信任情報$t = (t_I, t_C)$を生成する。(t_I, t_C)は、それぞれ以下のように構成される。

$$t_I = PkI$$

$$t_c = \{H(PkC_1), H(PkC_2), \cdots H(PkC_n)\}$$

ここで、ＰｋＩは、制御部１１が保持する検証鍵、PkC_iは発行者が「信用する」第三者（後述）による署名を検証するための検証鍵である。

【００３８】

図５は、本発明の一実施例の利用者装置の構成を示す。同図に示す利用者装置２は、制御部２１、格納部２２と、制御部２３、認証部２４、署名部２５、番号生成部２６、格納部２７から構成する耐タンパ装置２８を有する。各部の機能や内容が改竄されることを（利用者本人からも）防止する。このような耐タンパ装置２８として、ＩＣカードや、ネットワーク経由で構成され、第三者により厳重に管理されたサーバなどが利用可能である。

【００３９】

制御部２１は、耐タンパ装置２８に封入された制御部２６と共に、チケットの流通を安全に行うための制御を行う。制御部２１による制御の詳細については後述する。

格納部２２は、利用者が保持する署名付きデータの集合M_u及び発行者による署名付きの信任情報の集合T_uを格納する。これらの集合は、制御部２１により更新可能である。

【００４０】

制御部２３は、検証鍵ＰｋＵ，ＰｋＣ及び鍵証明書ＰｋＵ‖S_{PkC}（ＰｋＵ）を保持し、制御部２１と共に、チケットの流通を安全に行うための制御を行う。ここでＰｋＵは署名部２５が備えるS_{PkU}に対応する検証鍵であり、S_{PkC}は、ＩＣカード製造者もしくは、耐タンパサーバ管理者など、耐タンパ装置２８の安全性を保証する第三者により秘匿される署名関数である。即ち、署名関数S_{PkU}を含む耐タンパ装置２８は、署名関数S_{PkC}を保有する第三者により耐タンパ性が保証されている。制御部２３による制御の詳細については後述する。また、ＰｋＣは、S_{PkC}の検証鍵である。

【００４１】

認証部２４は、検証器Ｖを備える。

署名部２５は、署名関数S_{PkU}を備える。S_{PkU}は、利用者装置２毎にそれぞれ異なり、署名部２５により秘匿される。

番号生成部２６は、次番号r_Uを保持し、番号の払出しを要求されると、現在の番号r_Uの値を返却すると共に、r_Uをインクリメントする。

【００４２】

格納部２７は、マニフェストの集合$C_U = \{c_1, c_2, \cdots, c_n\}$及び番号の集合$R_U = \{r_1, r_2, \cdots, r_m\}$を格納する。これらの集合は、制御部２１により更新可能である。

図６は、本発明の一実施例の改札者装置の構成を示す。

同図に示す改札者装置３は、制御部３１、認証部３２、番号生成部３３、及び格納部３４から構成される。

【００４３】

制御部３１は、検証鍵ＰｋＶを備え、チケットの流通を安全に行うための制御を行う。制御部３１による制御の詳細については後述する。

認証部３２は、検証器Ｖを備える。

番号生成部３３は、次番号r_vを　保持し、番号の払出しを要求されると、r_vを返却すると共に、r_vをインクリメントする。

【００４４】

格納部３４は、番号の集合$R_V = \{r_1, r_2, \cdots, r_m\}$を格納する。これらの集合は、制御部３１により更新可能である。

図７は、本発明の一実施例の接続装置４の構成を示す。

同図に示す接続装置４は、通信部４１を有する。通信部４１は、発行者装置１、利用者装置２、改札者装置３間や利用者装置２相互間での一時的もしくは、永続的な通信手段を提供する。ここで、接続装置４としてＩＣカード挿入口を備えたキオスク端末や、ネットワークを介して相互接続された複数のＰＣなどが利用可能である。

【００４５】

上述したような構成を有する各装置を用いて、電子チケットの流通を安全に行う方式を以下において説明する。

以下で述べる流通方式における基本的な考え方は、以下のようなものである。

・チケット本体は、発行者による署名付きのデータ$m \| S_{PkI}$（ｍ）で表現されるものとする。ｍには、発行者がチケットの所有者に与える権利の内容が記述されているものとする。

【００４６】

・チケット発行者の署名S_{PkI}により、チケットの改竄は防止できる。

・チケット本体の複製は、特に禁止しない。

・チケット本体から、そのチケットに対応するマニフェスト$c_{(m,PkI)}$を生成できる。このマニフェストは、事実上チケットに１対１に対応する。

・マニフェストは、発行者が信用できる耐タンパ装置２８内の格納部２７に格納されることにより、「有効」なものとなる。

【００４７】

・発行者が信用できる耐タンパ装置とは、発行者が信用する者によって耐タンパ性が保証された装置である。発行者が信用する者は、信任情報t_Iにより規定される。

・チケットを消費もしくは、譲渡するためには、有効なマニフェストが必要である。

【００４８】

・有効なマニフェストは、対応するチケットの発行者のみが新規に作成可能である。

・１つの有効なマニフェストから、複数の有効なマニフェストを作成することを禁止する。即ち、利用者が勝手に有効なマニフェストを作成することを不可能にする。

【００４９】

以下、（１）チケット発行の場合、（２）チケット譲渡の場合、（３）チケット検証の場合、のそれぞれの場合に分けてチケットの流通方式を説明する。なお、各装置を跨がるそれぞれの通信は、接続装置４中の通信部４１を介するものとする。

（１）　チケット発行の場合：

以下は、発行者装置１から利用者装置２に対する接続装置４を介したチケット発行処理の流れである。

【００５０】

図８は、本発明の一実施例のチケット発行処理のシーケンスチャートである。

ステップ１０１）　制御部１１は、以下の手順によりｍ及びS_{PkI}（ｍ）を得て、署名付きデータであるところのチケット$m \| S_{PkI}$（ｍ）の生成を行う。

（ａ）　データ生成部１３によりデータｍを生成する。

（ｂ）　署名部１２にｍを与え、S_{PkI}（ｍ）を生成する。

【００５１】

ステップ１０２）　制御部１１は、マニフェスト生成部１４にチケット$m \| S_{PkI}$（ｍ）を与え、マニフェスト$c_{(m,PkI)}$を生成する。

ステップ１０３）　制御部１１は、以下の手順により信任情報ｔ及び署名関数

S_{PkI}（ｔ）を得て、署名付き信任情報ｔ‖S_{PkI}（ｔ）の生成を行う。

（ａ）　信任情報生成部１５により、信任情報ｔを生成する。ｔの構成は、前述の通りである。

【００５２】

（ｂ）　署名部１２に信任情報ｔを与え、署名S_{PkI}（ｔ）を生成する。

ステップ１０４）　制御部１１は、制御部２１にチケットｍ‖S_{PkI}（ｍ）と署名付き信任情報ｔ‖S_{PkI}（ｔ）を転送する。

ステップ１０５）　制御部２１は、チケットｍ‖S_{PkI}（ｍ）を格納部２２のM_Uに、署名付き信任情報ｔ‖S_{PkI}（ｔ）を格納部２２の信任情報の集合T_Uにそれぞれ追加して格納する。

【００５３】

ステップ１０６）　制御部２１は、制御部２３にセッション情報（s_1，s_2）の生成を依頼する。

制御部２３は、以下の手順により、セッション情報（s_1，s_2）を生成し、制御部２１に転送する。

（ａ）　番号生成部２６により、番号r_Uの払い出しを受ける。

【００５４】

（ｂ）　r_Uを格納部２７の番号集合R_Uに追加する。

（ｃ）　（s_1，s_2）＝（Ｈ（ＰｋＵ），r_U）を生成する。ここで、ＰｋＵは、制御部２１が保持する検証鍵である。

ステップ１０７）　制御部２１は、制御部１１にセッション情報（s_1，s_2）を転送する。

【００５５】

ステップ１０８）　制御部１１は、署名部１２が備えるS_{PkI}と制御部１１が保持する検証鍵ＰｋＩを用い、マニフェスト発行形式e_I＝（e_1，e_2，e_3，e_4，e_5）を得る。ここで、e_Iの各要素は以下の値をとる。

$e_1 = c_{(m,Pki)}$，

$e_2 = s_1$

$e_3 = s_2$

$e_4 = S_{PkI}(c_{(m,PkI)} \| s_1 \| s_2)$

$e_5 = PkI$

ステップ１０９）　制御部１１は、制御部２１にマニフェスト発行形式e_Iを転送する。

【００５６】

ステップ１１０）　制御部２１は、制御部２３にマニフェスト発行形式e_Iを転送し、e_I内のマニフェストの格納を依頼する。

ステップ１１１）　制御部２３は、認証部２４を用い、以下の式で全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１を介して、制御部１１に処理の中断の通知を行う。

【００５７】

$$e_2 = H(PkU) \quad (1)$$

$$e_3 \in R_U \quad (2)$$

$$V_{e5}(m \| S_{PkI}(m)) = 1 \quad (3)$$

$$V_{e5}(e_1 \| e_2 \| e_3 \| e_4) = 1 \quad (4)$$

上記の式（１）及び式（２）は、セッション情報の正当性の検証である。この検証により、他の利用者装置２宛のマニフェスト発行形式を格納すること、及びマニフェスト発行形式の再利用によってマニフェストを複製すること、などの不正を防止する。式（３）及び式（４）は、マニフェスト発行形式に対する署名の正当性の検証である。この検証により、チケットの発行者が署名したマニフェスト発行形式に含まれるマニフェスト以外を格納することを防止する。

【００５８】

ステップ１１２）　制御部２３は、格納部２７の番号集合R_Uからe_3（$= r_U$）を削除する。

ステップ１１３）　制御部２３は、格納部２７のマニフェストの集合C_Uにe_1（$= c_{(m,PkI)}$）を追加する。

ステップ１１４）　制御部２３は、制御部２１にe_1を転送し、処理の正常終了を通知する。

【００５９】

ステップ１１５）　制御部２１は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は、処理の正常終了を、制御部１１に通知する。

$$H(m \| S_{PkI}(m)) \in C_U \qquad (5)$$

上記の式（５）は、発行されたチケットに対応するマニフェストが格納部２７に格納されたことの検証である。この検証により、有効なマニフェストが合わせて発行されたこと、即ち、発行されたチケットが有効であることを確認する。

【００６０】

（２）　チケット譲渡の場合：

以下は、利用者装置２ａから利用者装置２ｂに対する接続装置４を介したチケット譲渡処理の流れである。

図９、図１０は、本発明の一実施例のチケット譲渡処理のシーケンスチャートである。

【００６１】

ステップ２０１）　制御部２１ａは、格納部２２ａが保持する署名付きデータの集合M_{Ua}から譲渡対象となるチケット$m \| S_{PkI}(m)$を抽出する。

ステップ２０２）　制御部２１ａは、格納部２２ａが保持するT_{Ua}から$m \| S_{PkI}(m)$の発行者による署名付き信任情報$t \| S_{PkI}(t)$を抽出する。

ステップ２０３）　制御部２１ａは、制御部２１ｂに$m \| S_{PkI}(m)$と$t \| S_{PkI}(t)$を転送する。

【００６２】

ステップ２０４）　制御部２１ｂは、$m \| S_{PkI}(m)$を格納部２２ｂの署名付きデータの集合M_{Ub}に、$t \| S_{PkI}(t)$を格納部２２の信任情報の集合T_{Ub}に、それぞれ格納する。

ステップ２０５）　制御部２１ｂは、制御部２３ｂにセッション情報（s_1，s_2）の生成を依頼する。制御部２３ｂは、以下の手順により（s_1，s_2）を生成し、制御部２１ｂに転送する。

【００６３】

（ａ）　番号生成部２６ｂにより番号r_{Ub}の払出しを受ける。

（ｂ）　r_{Ub}を格納部２７ｂの番号集合R_{Ub}に追加する。

（ｃ）　（s_1，s_2）＝（Ｈ（ＰｋＵｂ），r_{Ub}）を生成する。ここで、ＰｋＵｂは、制御部２１ｂが保持する検証鍵である。

ステップ２０６）　制御部２１ｂは、制御部２１ａに（s_1，s_2）を転送する。

【００６４】

ステップ２０７）　制御部２１ａは、制御部２３ａに（s_1，s_2）と譲渡対象チケットのハッシュＨ（ｍ‖S_{PkI}（ｍ））を転送する。

ステップ２０８）　制御部２３ａは、格納部２７ａに格納されたマニフェスト集合C_{Ua}について、以下の式が成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１ａに処理の失敗を通知する。

【００６５】

$$H(m \| S_{PkI}(m)) \in C_{Ua} \qquad (6)$$

上記の式（６）は、譲渡対象チケットに対応するマニフェスト$c_{(m,PkI)}$＝Ｈ（ｍ‖S_{PkI}（ｍ））が格納部２７ａに格納されていることの検証である。

ステップ２０９）　制御部２３ａは、署名部２５ａが備えるS_{PkUa}と制御部１１が保持する検証鍵ＰｋＵａ，ＰｋＣａ及び鍵証明書ＰｋＵａ‖S_{PkCa}（ＰｋＵａ）を用い、マニフェスト転送形式e_c＝（e_1，e_2，e_3，e_4，e_5，e_6，e_7）を得る。ここで、e_cの各要素は、以下の値となる。

【００６６】

$e_1 = c_{(m,PkI)}$

$e_2 = s_1$

$e_3 = s_2$

$e_4 = S_{PkUa}(c_{(m,PkI)} \| s_1 \| s_2)$

$e_5 = PkUa$

$e_6 = S_{PkCa}(PkUa)$

$e_7 = PkCa$

ステップ２１０）　制御部２３ａは、マニフェスト集合C_{Ua}から$c_{(m,PkI)}$を削除する。

【００６７】

ステップ２１１）　制御部２３ａは、制御部２１ａにe_Cを転送する。

ステップ２１２）　制御部２１ａは、制御部２１ｂにe_Cを転送する。

ステップ２１３）　制御部２１ｂは、制御部２３ｂにe_C，$t \| S_{PkI}$（ｔ），$m \| S_{PkI}$（ｍ）を転送し、e_C内のマニフェストの格納を依頼する。

ステップ２１４）　制御部２３ｂは、認証部２４ｂを用い、以下の式で全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１ｂに処理の中断を通知する。

【００６８】

$$e_2 = H(PkUb) \quad (7)$$

$$e_3 \in R_{Ub} \quad (8)$$

$$V_{ea}(e_1 \| e_2 \| e_3 \| e_4) = 1 \quad (9)$$

$$V_{er}(e_5 \| e_6) = 1 \quad (10)$$

$$H_{(er)} \in t_c \quad (11)$$

$$V_{t1}(m \| S_{PkI}(m)) = 1 \quad (12)$$

$$V_{t1}(t \| S_{PkI}(t)) = 1 \quad (13)$$

上記の式（７）及び式（８）は、セクション情報の正当性の検証である。この検証により、他の利用者装置２宛のマニフェスト転送形式を格納すること、及びマニフェスト転送形式の再利用により、マニフェストを複製すること、などの不正を防止する。

【００６９】

式（９）は、マニフェスト転送形式の署名者を特定するための検証であり、式（１０）は、該署名者の鍵証明書の検証であり、式（１１）は、当該鍵証明書の書名者が、信任情報中の信任情報中の信任対象として発行者により信任されていることの検証である。これらの検証により、発行者が信用する者によって当該マニフェスト転送形式の転送元の耐タンパ性が保証されていることを確認する。

【００７０】

式（１２）及び式（１３）は、当該信任情報に対する署名の正当性の検証である。この検証により、当該信任情報が当該チケットの署名者により正しく署名さ

れていることを確認する。

ステップ２１５）　制御部２３ｂは、格納部２７ｂの番号の集合R_{Ub}からe_3（＝r_{Ub}）を削除する。

【００７１】

ステップ２１６）　制御部２３ｂは、格納部２７ｂのマニフェスト集合C_{Ub}にe_1（＝$c_{(m,PkI)}$）を追加する。

ステップ２１７）　制御部２３ｂは、制御部２１ｂに処理の正常終了を通知する。

ステップ２１８）　制御部２１ｂは、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を、検証に成功した場合は、処理の正常終了を、制御部２１ａに通知する。

【００７２】

$$H(m \| S_{PkI}(m)) \in C_{Ub} \qquad (14)$$

上記の式（１４）は、譲渡されたチケットに対応するマニフェストが格納部２７ｂに格納されたことの検証である。この検証により、有効なマニフェストが合わせて転送されたこと、即ち、譲渡されたチケットが有効であることを確認する。

【００７３】

（３）　チケット消費の場合：

以下は、利用者装置２から改札者装置３に対する、接続装置４を介したチケット消費処理の流れである。

図１１は、本発明の一実施例のチケット消費のシーケンスチャートである。

ステップ３０１）　制御部２１は、格納部２２が保持する署名付きデータの集合M_Uから消費対象となるチケット$m \| S_{PkI}(m)$を抽出する。

【００７４】

ステップ３０２）　制御部２１は、格納部２２が保持する署名付き信任情報の集合T_Uから$m \| S_{PkI}(m)$の発行者による署名付き信任情報$t \| S_{PkI}(t)$を抽出する。

ステップ３０３）　制御部２１は、制御部３１に$m \| S_{PkI}(m)$と$t \| S_{Pk}$

$_I$（ｔ）を転送する。

【００７５】

ステップ３０４）　制御部３１は、以下の手順によりセッション情報（s_1，s_2）を生成する。

（ａ）　番号生成部３３により番号r_Vの払出しを受ける。

（ｂ）　r_Vを格納部３４の番号集合R_Vに追加する。

（ｃ）　（s_1，s_2）＝（Ｈ（ＰｋＶ），r_V）を生成する。ＰｋＶは制御部３１が保持する検証鍵である。

【００７６】

ステップ３０５）　制御部３１は、制御部２１にセッション情報（s_1，s_2）を転送する。

ステップ３０６）　制御部２１は、制御部２３に、（s_1，s_2）と消費対象チケットのハッシュＨ（ｍ‖S_{PkI}（ｍ））を転送する。

ステップ３０７）　制御部２３は、格納部２７に格納されたマニフェスト集合C_Uについて、以下の式が成立することを検証する。検証に失敗した場合には、以後の処理を中断し、制御部２１に処理の失敗を通知する。

【００７７】

$$H(m \| S_{PkI}(m)) \in C_U \qquad (15)$$

上記の式（１５）は、消費対象チケットに対応するマニフェスト$c_{(m,PkI)}$＝Ｈ（ｍ‖S_{PkI}（ｍ））が格納部２７に格納されていることの検証である。

ステップ３０８）　制御部２３は、署名部２５が備える署名関数S_{PkU}と制御部１１が保持する検証鍵ＰｋＵ，ＰｋＣ及び鍵証明書ＰｋＵ‖S_{PkC}（ＰｋＵ）を用い、マニフェスト転送形式e_C＝（e_1，e_2，e_3，e_4，e_5，e_6，e_7）を得る。ここで、e_Cの各要素は以下の値をとる。

【００７８】

$e_1 = c_{(m,PkI)}$

$e_2 = s_1$

$e_3 = s_2$

$e_4 = S_{PkU}(c_{(m,PkI)} \| s_1 \| s_2)$

e_5 ＝ＰｋＵ

e_6 ＝S_{PkC}（ＰｋＵ）

e_7 ＝ＰｋＣ

ステップ３０９）　制御部２３は、マニフェスト集合C_Uから$c_{(m,PkI)}$を削除する。

【００７９】

ステップ３１０）　制御部２３は、制御部２１にe_Cを転送する。

ステップ３１１）　制御部２１は、制御部３１にe_Cを転送する。

ステップ３１２）　制御部３１は、認証部３２を用い、以下の式の全てが成立することを検証する。検証に失敗した場合、以後の処理を中断し、制御部２１に処理の中断を通知する。

【００８０】

$$e_2 = H(PkV) \quad (16)$$

$$e_3 \in R_V \quad (17)$$

$$V_{cb}(e_1 \| e_2 \| e_3 \| e_4) = 1 \quad (18)$$

$$V_{e7}(e_5 \| e_6) = 1 \quad (19)$$

$$H(e_r) \in t_C \quad (20)$$

$$V_{tI}(m \| S_{PkI}(m)) = 1 \quad (21)$$

$$V_{tI}(t \| S_{PkI}(t)) = 1 \quad (22)$$

上記の式（１６）及び式（１７）は、セッション情報の正当性の検証である。この検証により、他の改札者装置３宛のマニフェスト転送形式を格納すること、及び自分宛のマニフェスト転送形式の再利用により、マニフェストを複製すること、などの不正を防止する。

【００８１】

式（１８）は、マニフェスト転送形式の署名者を特定するための検証であり、式（１９）は、当該署名者の鍵証明書の検証であり、式（２０）は、当該鍵証明書の署名者が信任情報中の信任対象として発行者により信任されていることの検証である。これらの検証により、発行者が信用する者によって当該マニフェスト転送形式の転送元の耐タンパ性が保証されていることを確認する。

【００８２】

式（２１）及び式（２２）は、当該信任情報に対する署名の正当性の検証である。この検証により、当該信任情報が当該チケットの署名者により正しく署名されていることを確認する。

ステップ３１３）　制御部３１は、格納部３４のR_Vからe_3（$=r_V$）を削除する。

【００８３】

ステップ３１４）　制御部３１は、以下の式が成立することを検証する。検証に失敗した場合は、処理の中断を制御部２１に通知する。検証に成功した場合は、mに対応するサービスを消費者に提供する。

$$e_1 = H(m \| S_{PkI}(m)) \qquad (23)$$

上記の式（２３）は、消費されたチケットに対応するマニフェストが転送されたことの検証である。この検証により、有効なマニフェストが併せて転送されたこと、即ち、有効なチケットが消費されたことを確認する。

【００８４】

また、前述の図３に示す発行者装置１、利用者装置２、改札装置３の各構成要素をプログラムとして構築し、発行者装置、利用者装置、改札装置として利用されるコンピュータに接続されるディスク装置や、フロッピーディスクやＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際に、各コンピュータにインストールすることにより容易に本発明を実現できる。

【００８５】

なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において種々変更・応用が可能である。

【００８６】

【発明の効果】

上述のように、本発明によれば、データの署名者の意図した数だけマニフェストをデータ蓄積システムのマニフェスト格納部に格納し、当該署名者以外が該マニフェストを新たに格納することを防止する、該マニフェストの数を越えて有効なデータが存在することを防止する、当該署名者が信用する経路のみを介してマ

ニフェストを移送することが可能となる。

【００８７】

チケットを本発明のデータ蓄積システムのデータとして用いることにより、チケット自体を耐タンパ装置に格納することなしに、チケットの有効な複製数を一定に保つことが可能となる。

また、プログラムを本発明におけるデータとして用い、当該プログラムの実行ライセンスをマニフェストとして用いることにより、不当に複製された当該プログラムの実行を防止することが可能となる。

【００８８】

また、音楽データや画像データを本発明におけるデータとして用い、当該データの鑑賞権をマニフェストとして用いることにより、不当に複製された当該データの鑑賞を防止することが可能となる。

さらに、データを鑑賞する毎に当該データを「消費（実施例における（３））」することにより、利用毎の課金システム（pay per view　課金）などに利用することが可能である。

【図面の簡単な説明】

【図１】

本発明の原理を説明するための図である。

【図２】

本発明の原理構成図である。

【図３】

本発明のデータ蓄積システムの全体構成図である。

【図４】

本発明の一実施例の発行者装置の構成図である。

【図５】

本発明の一実施例の利用者装置の構成図である。

【図６】

本発明の一実施例の改札者装置の構成図である。

【図７】

本発明の一実施例の接続装置の構成図である。

【図８】

本発明の一実施例のチケット発行処理のシーケンスチャートである。

【図９】

本発明の一実施例のチケット譲渡処理のシーケンスチャート（その１）である。

【図１０】

本発明の一実施例のチケット譲渡処理のシーケンスチャート（その２）である。

【図１１】

本発明の一実施例のチケット消費処理のシーケンスチャートである。

【符号の説明】

１　発行者装置

２　利用者装置

３　改札者装置

４　接続装置

１１　制御部

１２　署名部

１３　データ生成部

１４　マニフェスト生成部

１５　信任情報生成部

２１　制御部

２２　格納部

２３　制御部

２４　認証部

２５　署名部

２６　番号生成部

２７　格納部

３１　制御部

３２　認証部

３３　番号生成部

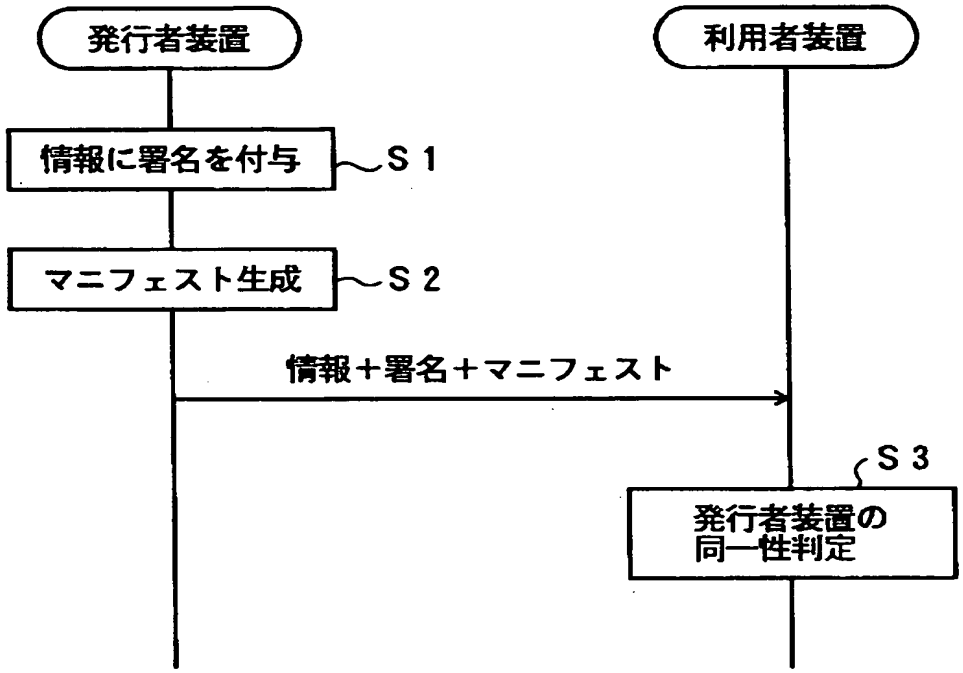
３４　格納部

４１　通信部

【書類名】　図面

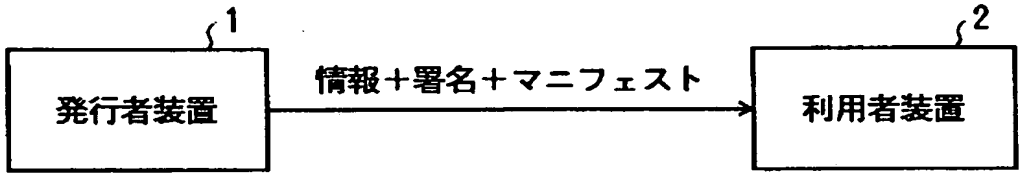
【図１】

本発明の原理を説明するための図



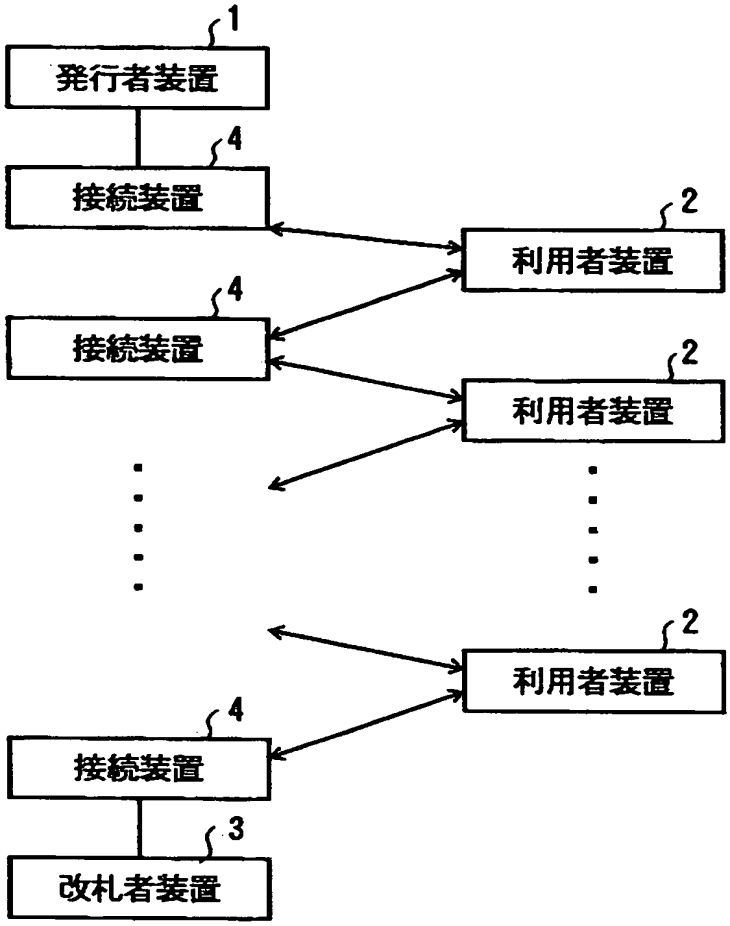
【図２】

本発明の原理構成図



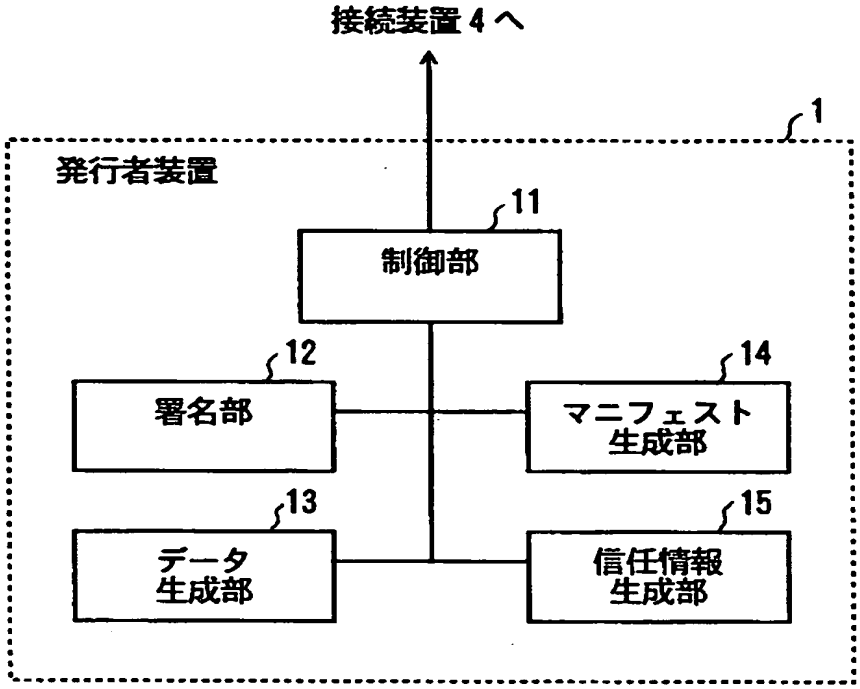
【図３】

本発明のデータ蓄積システムの全体構成図



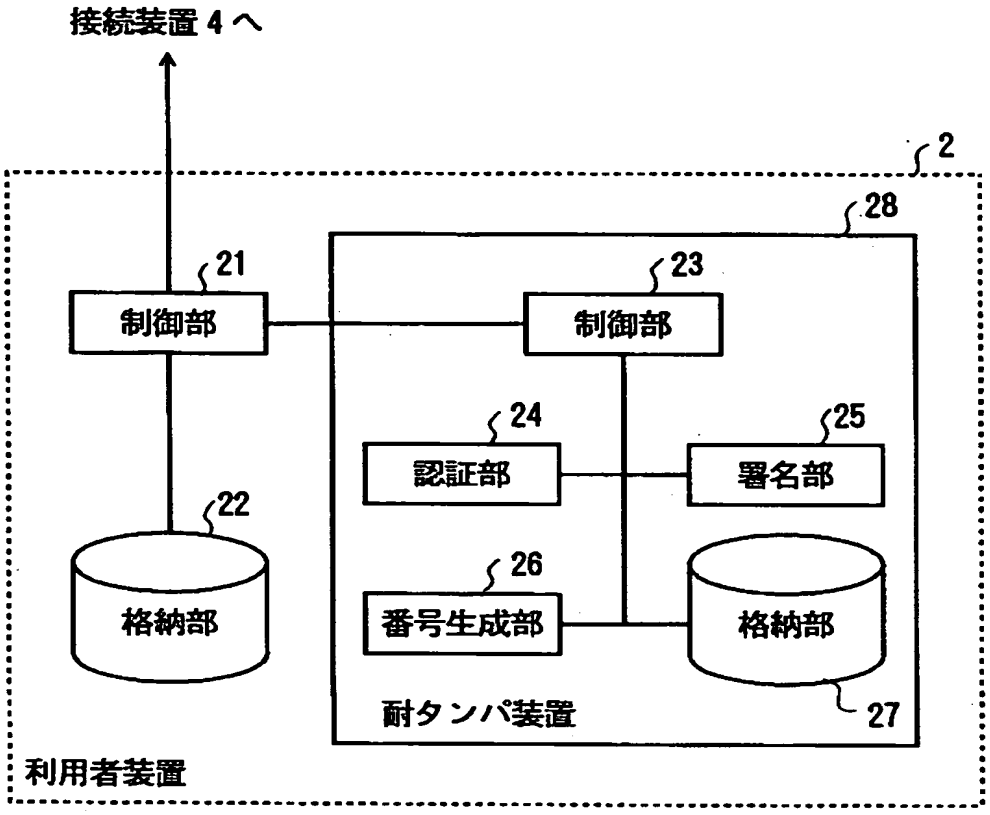
【図４】

本発明の一実施例の発行者装置の構成図



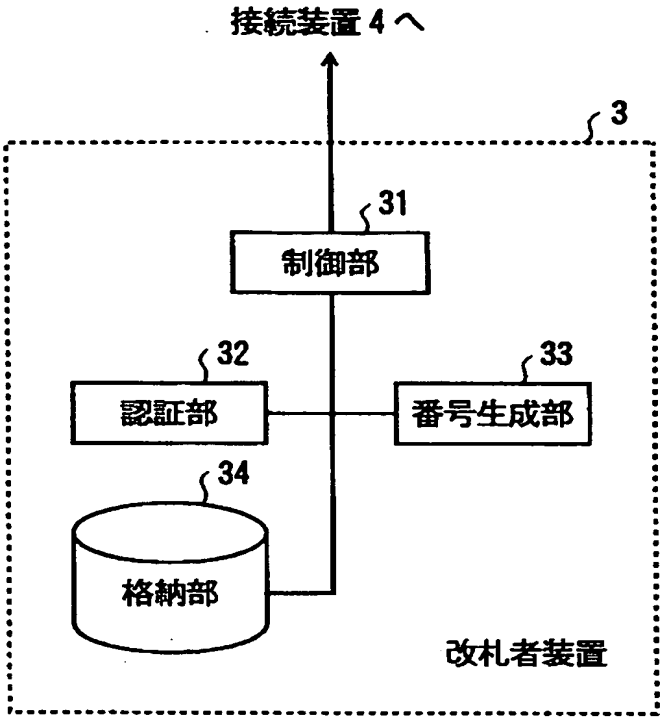
【図５】

本発明の一実施例の利用者装置の構成図



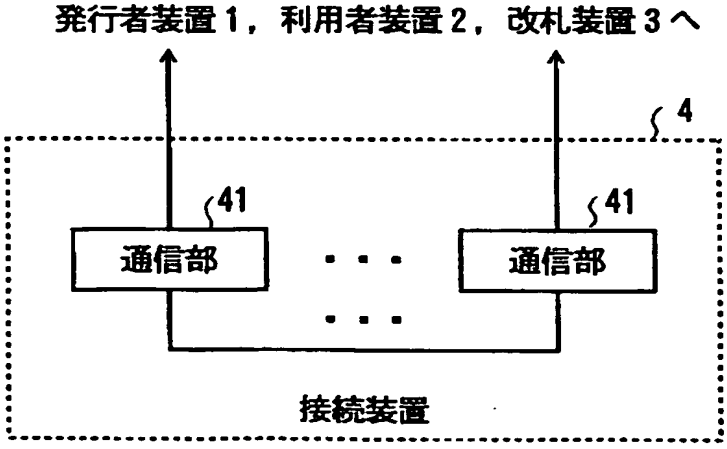
【図６】

本発明の一実施例の改札者装置の構成図



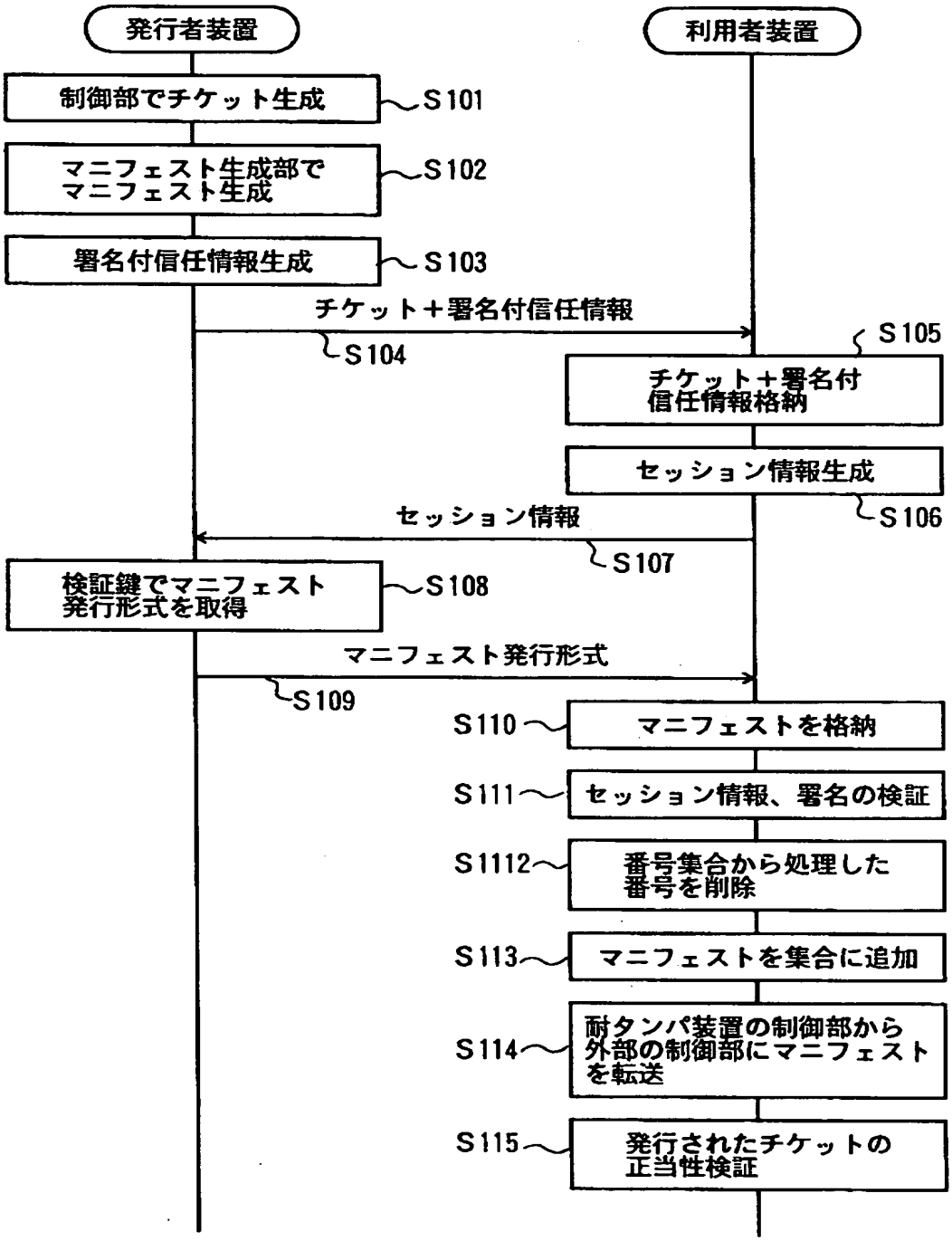
【図７】

本発明の一実施例の接続装置の構成図



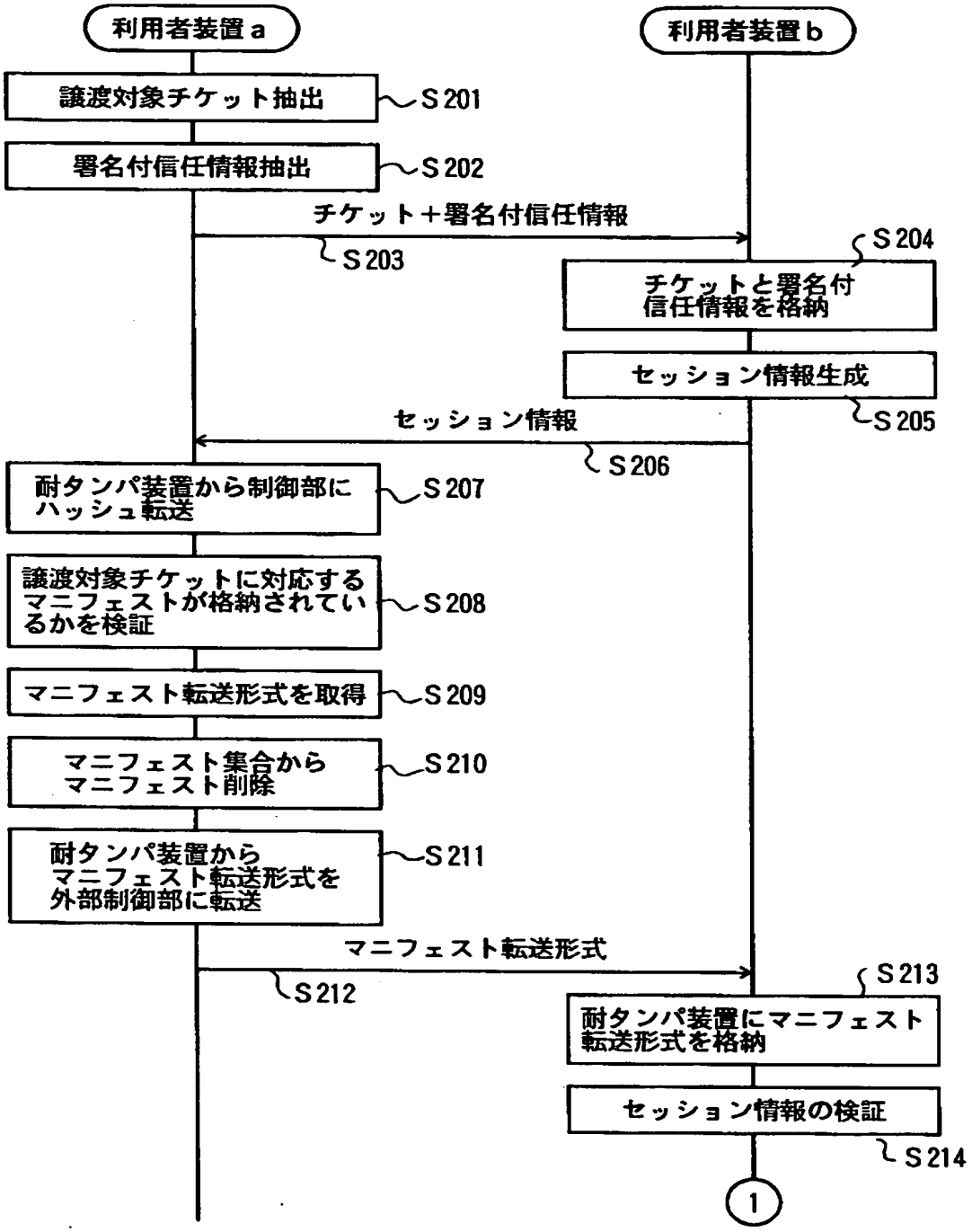
【図８】

本発明の一実施例のチケット発行処理のシーケンスチャート



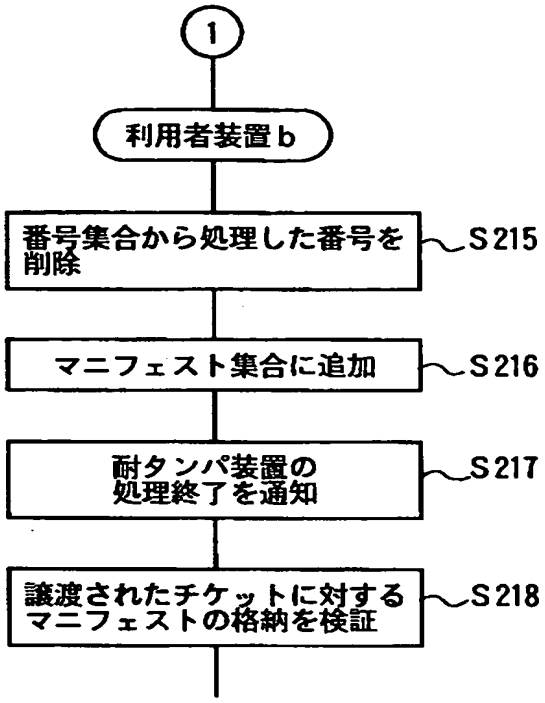
【図９】

本発明の一実施例のチケット譲渡処理のシーケンスチャート（その１）



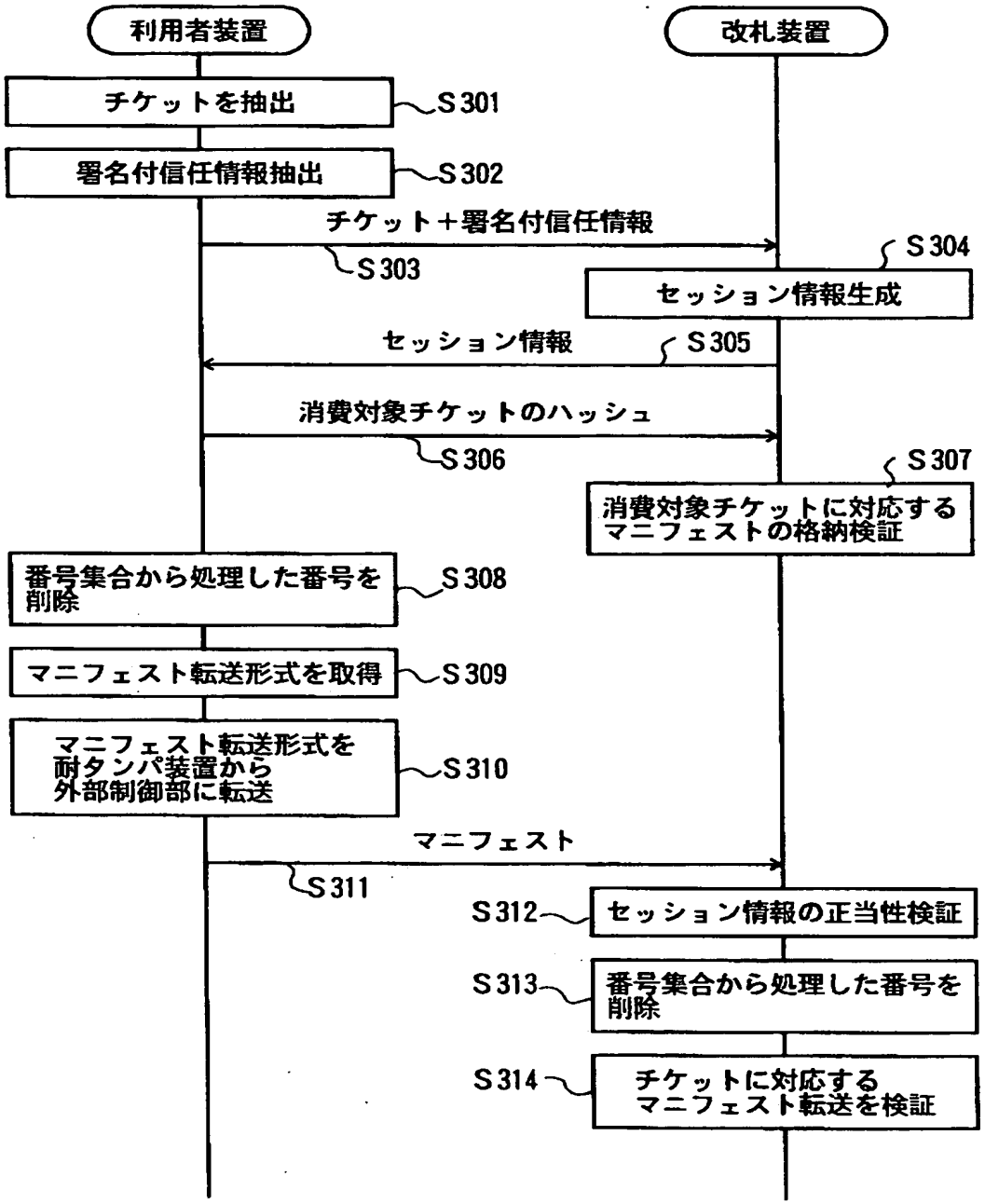
【図１０】

本発明の一実施例のチケット譲渡処理のシーケンスチャート（その２）



【図１１】

本発明の一実施例のチケット消費処理のシーケンスチャート



【書類名】　　要約書

【要約】

【課題】　データの有効な複製数を一定以下に保つことを保証しつつ、記述の正当性の検証を含む複製に関する有効性以外の検証をすべて耐タンパ装置に委ねることなく、処理速度や記憶容量等の処理負荷を低減させるデータ蓄積方法及びシステム及びデータ蓄積プログラムを格納した記憶媒体を提供する。

【解決手段】　本発明は、電子的な情報の発行者装置により該電子的な情報に署名した第１の情報を付与し、発行者装置により電子的な情報と対応するマニフェストの第２の情報を生成して、第１の情報に付与し、電子的な情報利用装置において、第１の情報と第２の情報を用いて電子的な情報の発行者装置の同一性を判定し、電子的な情報の複製を防止する。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９５年　９月２１日
［変更理由］　住所変更
住　所　東京都新宿区西新宿三丁目１９番２号
氏　名　日本電信電話株式会社

２．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社